特 許 協 力 条 約

PCT

特許性に関する国際予備報告（特許協力条約第二章）

（法第１２条、法施行規則第56条）
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号 Ｐ３２０９１－Ｐ０	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ０３／１３２１８	国際出願日 (日.月.年) １５．１０．２００３	優先日 (日.月.年) １７．１０．２００２
国際特許分類（ＩＰＣ） Ｉｎｔ．Ｃｌ’ Ｈ０４Ｌ１２／５６		
出願人（氏名又は名称） 松下電器産業株式会社		

１．この報告書は、ＰＣＴ３５条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

２．この国際予備審査報告は、この表紙を含めて全部で ６ ページからなる。

３．この報告には次の附属物件も添付されている。

a [x] 附属書類は全部で １８ ページである。

[x] 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則70.16及び実施細則第６０７号参照）

[ ] 第Ｉ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b [ ] 電子媒体は全部で ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、コンピュータ読み取り可能な形式による配列表又は配列表に関連するテーブルを含む。（実施細則第８０２号参照）

４．この国際予備審査報告は、次の内容を含む。

[x] 第Ｉ欄 国際予備審査報告の基礎
[ ] 第Ⅱ欄 優先権
[ ] 第Ⅲ欄 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
[ ] 第Ⅳ欄 発明の単一性の欠如
[x] 第Ⅴ欄 ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
[ ] 第Ⅵ欄 ある種の引用文献
[ ] 第Ⅶ欄 国際出願の不備
[ ] 第Ⅷ欄 国際出願に対する意見

国際予備審査の請求書を受理した日 ０５．０２．２００４	国際予備審査報告を作成した日 ２０．０５．２００４
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） ５Ｘ ３０４７ 玉木 宏治 電話番号 ０３－３５８１－１１０１ 内線 ３５９６

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００４年１月）

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／１３２１８

第Ⅰ欄　報告の基礎

１．この国際予備審査報告は、下記に示す場合を除くほか、国際出願の言語を基礎とした。

☐ この報告は、＿＿＿＿＿＿語による翻訳文を基礎とした。
それは、次の目的で提出された翻訳文の言語である。
☐ ＰＣＴ規則12.3及び23.1(b)にいう国際調査
☐ ＰＣＴ規則12.4にいう国際公開
☐ ＰＣＴ規則55.2又は55.3にいう国際予備審査

２．この報告は下記の出願書類を基礎とした。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☐ 出願時の国際出願書類

☒ 明細書
第 1-76 ページ、　出願時に提出されたもの
第 ＿＿＿＿ ページ*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿ ページ*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの

☒ 請求の範囲
第 ＿＿＿＿ 項、　出願時に提出されたもの
第 ＿＿＿＿ 項*、　ＰＣＴ１９条の規定に基づき補正されたもの
第 52-98 項*、 １４．０５．２００４ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿ 項*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの

☒ 図面
第 1-38 ページ/~~図~~、　出願時に提出されたもの
第 ＿＿＿＿ ページ／図*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿ ページ／図*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

３．☒ 補正により、下記の書類が削除された。

☐ 明細書　第 ＿＿＿＿ ページ
☒ 請求の範囲　第 1-51 項
☐ 図面　第 ＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること）
☐ 配列表に関連するテーブル（具体的に記載すること）

４．☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)）

☐ 明細書　第 ＿＿＿＿ ページ
☐ 請求の範囲　第 ＿＿＿＿ 項
☐ 図面　第 ＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること）
☐ 配列表に関連するテーブル（具体的に記載すること）

＊４．に該当する場合、その用紙に "superseded" と記入されることがある。

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／１３２１８

第Ⅴ欄　新規性、進歩性又は産業上の利用可能性についての法第１２条（ＰＣＴ３５条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（Ｎ）

請求の範囲　52-98　有
請求の範囲　　無

進歩性（ＩＳ）

請求の範囲　68, 70, 71, 74, 94-98　有
請求の範囲　52-67, 69, 72, 73, 75-93　無

産業上の利用可能性（ＩＡ）

請求の範囲　52-98　有
請求の範囲　　無

２．　文献及び説明（ＰＣＴ規則70.7）

文献１：ＪＰ　２００２－２０２７２０　Ａ（株式会社東芝）
２００２．０７．１９　要約

文献２：ＪＰ　２０００－３４１３２４　Ａ（株式会社エヌ・ティ・ティ・データ）　２０００．１２．０８　第0002段落，第0003段落

文献３：ＪＰ　７－７９２５２　Ａ（富士通株式会社）
１９９５．０３．２０　要約

文献４：ＪＰ　８－１３０５４３　Ａ（日本電信電話株式会社）
１９９６．０５．２１　要約

文献５：ＪＰ　２０００－２９９６８６　Ａ（日本電気株式会社）
２０００．１０．２４　要約

文献６：ＪＰ　２００２－２６９０６　Ａ（三菱電機株式会社）
２００２．０１．２５　第0036段落，第0037段落

文献７：ＪＰ　７－２９７８３１　Ａ（住友電気工業株式会社）
１９９５．１１．１０　第0038段落

文献８：高田　学也，三輪　芳久，“特集２　インターネットの基盤「ＩＰを知る」”，日経ネットワーク，日経ＢＰ社，第30号，２００２．０９．２２，pp. 124-139
“役割３　パケットを分割する　通る回線に合わせて大きさを調整”(pp. 132-135)

文献９：ＪＰ　１１－１９６０８１　Ａ（株式会社高度移動通信セキュリティ技術研究所）　１９９９．０７．２１　第0003段落

補充欄

いずれかの欄の大きさが足りない場合

第 V.2　欄の続き

文献１０：山本　喜一，西野　謙一，高橋　哲也，「通信コスト削減の武器としてのVPN」，INTEROP MAGAZINE，ソフトバンクパブリッシング株式会社，第９巻，第８号，１９９９．１０．０１，pp. 44-51
p. 48左欄第32行目から第35行目

文献１１：ＪＰ　２００２－２１７９６１　Ａ（富士通株式会社）
２００２．０８．０２　請求項２

文献１２：ＪＰ　２００１－１８６１７３　Ａ（松下電器産業株式会社）
２００１．０７．０６　第0153段落

文献１３：ＪＰ　２００２－２３２９５５　Ａ（株式会社デンソー）
２００２．０８．１６　請求項１－３

文献１４：ＪＰ　２００１－８６１１０　Ａ（東洋通信機株式会社）
２００１．０３．３０　第0005段落，第９図

・請求の範囲　５２－５４，６５－６７，７５－７７，８０－８２
上記文献１，２のそれぞれには，送信装置と受信装置との間で，鍵交換を行い，当該鍵交換によって交換された鍵に基づいて，データを暗号化して送受信することが記載されている．
そして，送信アドレスなどの送信関連情報，MACアドレスなどの送受信管理情報などを用いて，パケットを生成することは，IP網において，一般的に行われていることである．
また，文献３，４には，バッファの蓄積量がしきい値を超えると，当該バッファからのデータを優先的に出力することが記載されている．
蓄積量がしきい値を超えたとき，データを優先的に出力して，蓄積量がしきい値を下回るように制御することは，蓄積量がしきい値を超えないように制御することに他ならない．
上記文献５には，パケットを複数のクラスのキューに蓄積し，前記クラスに割り当てられた帯域情報に基づいて，各キューに蓄積されたパケットを出力することが記載されている．

・請求の範囲　５５－６４
上記文献６には，重要度の高いデータは暗号化し，重要度の低いデータは暗号化しないで送信することが記載されている．

データの転送レートが所定の値より小さくならないように制御することは，シェーピング等で一般的に行われていることである．

補充欄

いずれかの欄の大きさが足りない場合

第 V.2　欄の続き

・請求の範囲　６０
上記文献７には，残り蓄積可能時間を超えないように，すなわち，蓄積される時間があらかじめ決めた値より小さくなるように，データを出力することが記載されている．

・請求の範囲　６１－６４，７９
上記文献８には，送信装置から受信装置までの伝送路において伝送可能な最大パケット長を調査して，当該最大パケット長でデータを伝送することが記載されている．
そして，伝送するパケットのパケット長や，エラー訂正用のデータをパケットに付加することは，一般的に行われていることである．

・請求の範囲　６９，７３，９０，９３
上記文献９には，鍵を一定時間使用すると，鍵の更新を行うことが記載されている．
どのようなプロトコルにおいて，一定時間毎に鍵を更新するかは，当該技術分野の専門家であれば，適宜決定できた設計的事項であり，プロトコルとして周知のRTPを採用することに格別の困難性は認められない．

・請求の範囲　７２，９２
上記文献１０には，一定のデータ量毎に鍵を更新することが記載されている．
どのようなプロトコルにおいて，一定のデータ量毎に鍵を更新するかは，当該技術分野の専門家であれば，適宜決定できた設計的事項であり，プロトコルとして周知のHTTPを採用することに格別の困難性は認められない．

・請求の範囲　７８
上記文献１１には，複数のキューから均等に，パケットを出力することが記載されている．

・請求の範囲　８３，８４
上記文献１２には，パケットの優先度のためのフィールドとして，IPv4パケットのTOSフィールド，IPv6パケットのトラヒッククラスのフィールドを用いることが記載されている．

・請求の範囲　８５－８９
上記文献１３には，移動端末の位置情報に基づいて認証を行い，認証の結果が否であればパスワードによる認証を行うことが記載されている．
そして，パスワードによる認証に代えて，証明書等で認証を行うように構成することは，当該技術分野の専門家であれば容易に成し得たことである．

補充欄

いずれかの欄の大きさが足りない場合

第 V.2　欄の続き

・請求の範囲　９１
上記文献１４には，送信パケットに鍵の変更タイミングを付加することが記載されている．

・請求の範囲　６８
上記文献１－１４のいずれにも，暗号鍵を示す情報を，送信フレームの送信から当該送信フレームに対応する受信フレームの受信までの時間より前に送信することは記載も示唆もされていない．

・請求の範囲　７０，７１，７４，９６，９７
上記文献１－１４のいずれにも，鍵更新のタイミングをシーケンス番号に同期したタイミングとすること，HTTPリクエスト毎に更新すること，エラー訂正マトリックスの終点または始点に同期したタイミングとすること，該タイミングを，ポート番号の変化によって通知することは記載も示唆もされていない．

・請求の範囲　９４，９５
上記文献１－１４のいずれにも，パケットの片道もしくは往復の伝播遅延時間や，スクランブルして伝送するモードであるか否かに基づいて認証を行うことは記載も示唆もされていない．

・請求の範囲　９８
上記文献１－１４のいずれにも，DTCP方式のコピー制御情報は，送信パケットに暗号化モード情報を付加することで伝送することは，記載も示唆もされていない．

請求の範囲

1. (削除)
2. (削除)
3. (削除)
4. (削除)
5. (削除)
6. (削除)
7. (削除)
8. (削除)
9. (削除)
10. (削除)
11. (削除)
12. (削除)
13. (削除)
14. (削除)
15. (削除)
16. (削除)
17. (削除)
18. (削除)
19. (削除)
20. (削除)
21. (削除)
22. (削除)
23. (削除)
24. (削除)
25. (削除)

２６．（削除）
２７．（削除）
２８．（削除）
２９．（削除）
３０．（削除）
３１．（削除）
３２．（削除）
３３．（削除）
３４．（削除）
３５．（削除）
３６．（削除）
３７．（削除）
３８．（削除）
３９．（削除）
４０．（削除）
４１．（削除）
４２．（削除）
４３．（削除）
４４．（削除）
４５．（削除）
４６．（削除）
４７．（削除）
４８．（削除）
４９．（削除）
５０．（削除）
５１．（削除）

５２．（追加） 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも１つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

前記復号鍵を用いて前記受信データを復号する復号手段と、

前記パケット化手段にて生成された第１のパケットを一時的に蓄積する第１のキュー手段と、

前記パケット化手段にて生成された第２のパケットを一時的に蓄積する第２のキュー手段と、

前記送信条件設定情報に基づいて、前記第１のキュー手段に蓄積された前記第１のパケットおよび前記第２のキュー手段に蓄積された前記第２のパケットのいずれを送信するかを制御する送信キュー制御手段と、

前記第１のキュー手段から出力された第１のパケットおよび第２のキュー手段から出力された第２のパケットをフレーム化することによって送信フレームを生成するフレーム化手段と、

受信フレームから前記受信パケットを抽出するフレーム受信手段と

を備え、

前記送信キュー制御手段は、前記第２のキュー手段に蓄積された前記第２のパケットの量が所定の量を超えないように前記第２のキュー手段に蓄積された前記第２のパケットが出力されるように、前記第１のキュー手段および前記第２のキュー手段を制御する、パケット送受信装置。

５３．（追加）　前記パケット化手段は、第１のパケット化手段と、第２のパケット化手段とを含み、

前記第１のパケット化手段は、前記送信条件設定情報および前記認証・鍵交換関連情報の少なくとも一つの情報を用いて前記第１のパケットを生成し、

前記第２のパケット化手段は、前記送信条件設定情報と、前記認証・鍵交換関連情報と、前記暗号化送信データとの少なくとも一つの情報を用いて前記第２のパケットを生成する、請求の範囲第５２項に記載のパケット送受信装置。

５４．（追加）　前記パケット化手段は、前記暗号化送信データを所定の大きさに変換し、ＩＥＴＦでＩＰｖ４またはＩＰｖ６として規定されているＩＰヘッダを付加し、

前記第１のパケット化手段はソフトウエアによって構成され、前記第２のパケット化手段はハードウエアによって構成される、請求の範囲第５３項に記載のパケット送受信装置。

５５．（追加）　前記送信データを優先データと一般データとに分離するデータ

分離手段をさらに備え、

前記暗号化手段は、前記優先データを暗号化し、

前記第１のパケット化手段は、前記一般データを用いて第１のパケットを生成する、請求の範囲第５３項に記載のパケット送受信装置。

５６．（追加） 前記第１のパケット化手段は、ＩＥＴＦ文書で規定されているデータ処理プロトコルであるＲＴＣＰ，ＲＴＳＰ，ＨＴＴＰ、ＴＣＰ、ＵＤＰ、ＩＰのうちの少なくとも１つのヘッダを付加する、請求の範囲第５５項に記載のパケット送受信装置。

５７．（追加） 前記第２のパケット化手段は、データにシーケンス番号を付加するか、または、ＩＥＴＦ文書で規定されているデータ処理プロトコルであるＲＴＰ，ＵＤＰ、ＨＴＴＰ、ＴＣＰ、ＩＰのうちの少なくとも１つのヘッダを付加する、請求の範囲第５５項に記載のパケット送受信装置。

５８．（追加） 前記優先データは、ＳＭＰＴＥ ２５９Ｍ規格で規定された非圧縮ＳＤ方式信号、または、ＳＭＰＴＥ ２９２Ｍ規格で規定された非圧縮ＨＤ形式、または、ＩＥＣ ６１８８３規格で規定されたＩＥＥＥ１３９４によるＤＶまたはＭＰＥＧ－ＴＳの伝送ストリーム形式、または、ＤＶＢ－ＡＳＩによるＭＰＥＧ－ＴＳ形式、ＭＰＥＧ－ＰＳ形式、ＭＰＥＧ－ＥＳ形式、ＭＰＥＧ－ＰＥＳ形式の内の少なくとも一つのデータストリーム形式またはデータファイル形式である、請求の範囲第５５項に記載のパケット送受信装置。

５９．（追加） 前記優先データのデータレートが所定の値より小さくならないように、前記送信キュー制御手段は前記第１のキュー手段および前記第２のキュー手段を制御する、請求の範囲第５５項に記載のパケット送受信装置。

６０．（追加） 前記送信キュー制御手段は、前記優先データが前記第２のキュー手段に蓄積される時間があらかじめ決めた値より常に小さくなるように、前記送信キュー制御手段は前記第１のキュー手段および前記第２のキュー手段を制御する、請求の範囲第５９項に記載のパケット送受信装置。

６１．（追加） 前記第２のパケット化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、前記第２のパケットのパケットヘッダを生成するパケットヘッダ生成手段と、前記パケットヘッダと前記バッファから出力されるペイロードとを組み合わせてパケットを合成するパケット合成手段とを含み、

前記パケットヘッダ生成手段は前記第２のパケットのペイロード長を指定して、前記バッファ手段に蓄積されたデータを読み出して、前記パケット合成手段に入力する、請求の範囲第５９項に記載のパケット送受信装置。

６２．（追加） 前記第２のパケット化手段は、前記優先データから抽出したデータを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、パケット化情報を用いてパケットヘッダを生成するパケットヘッダ生成手段と、前記パケットヘッダとペイロードとを組み合わせてパケットを生成するパケット生成手段とを含み、

前記カウンタ手段は前記バッファ手段からペイロード長に相当するデータを読み出すための制御データを出力する、請求の範囲第５９項に記載のパケット送受信装置。

６３．（追加） 前記第２のパケット化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、パケット化情報

を用いてパケットヘッダを生成するパケットヘッダ生成手段と、前記データにエラー訂正を付加するエラー訂正付加手段手段と、前記パケットヘッダと前記エラー訂正を付加したデータとを合成するパケット合成手段とを含み、

前記カウンタ手段は前記バッファ手段よりペイロード長に相当するデータを読み出すための制御データを出力する、請求の範囲第５９項に記載のパケット送受信装置。

６４．（追加） 前記優先データおよび前記一般データが処理されるレイヤよりも下位レイヤの受信フレームを処理するレイヤにおいて、前記受信フレームに含まれる受信パケットの通信プロトコルヘッダから前記優先データと前記一般データを選別して、前記優先データの処理と前記一般データの処理を独立に行う、請求の範囲第５９項に記載のパケット送受信装置。

６５．（追加） 前記第２のパケット化手段は、エラー訂正符号付加手段を含む、請求の範囲第５３項に記載のパケット送受信装置。

６６．（追加） 前記エラー訂正符号付加手段で用いられるエラー訂正符号の方式は、リードソロモン方式、あるいはパリティ方式である、請求の範囲第６５項に記載のパケット送受信装置。

６７．（追加） 前記暗号化鍵を示す情報は、前記フレーム化手段において前記暗号化鍵で暗号化された送信パケットを出力するより前に、前記暗号化鍵の復号情報を前記フレーム化手段から出力する、請求の範囲第５３項に記載のパケット送受信装置。

６８．（追加） 前記暗号化鍵を示す情報は、前記暗号化鍵を用いて生成された

前記暗号化送信データを含む送信パケットが送信されるときよりも、前記送信フレームの送信から前記送信フレームに対応する受信フレームの受信までの時間より前に送信される、請求の範囲第６７項に記載のパケット送受信装置。

６９．（追加） 前記第２のパケット化手段は、暗号鍵切替手段を含み、前記暗号鍵切替手段に入力される暗号鍵を指定されたタイミングで切り替えながら前記暗号化手段に入力し、前記暗号化手段における暗号化鍵を指定の間隔で切替る、請求の範囲第５３項に記載のパケット送受信装置。

７０．（追加） 前記暗号鍵切替に用いるタイミングとしては、前記パケットヘッダ生成手段の出力であるパケットヘッダ内の所定のシーケンス番号に同期して発生したタイミングである、請求の範囲第６９項に記載のパケット送受信装置。

７１．（追加） 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、ＨＴＴＰリクエスト毎に更新される、請求の範囲第６９項に記載のパケット送受信装置。

７２．（追加） 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、一定のデータ量毎に変化される、請求の範囲第６９項に記載のパケット送受信装置。

７３．（追加） 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＲＴＰを使用している場合、予め決められた期間内に更新される、請求の範囲第６９項に記載のパケット送受信装置。

７４．（追加） 前記暗号鍵切替に用いるタイミングとしては、エラー訂正マト

リックスの終点または始点に同期して発生したタイミングである、請求の範囲第６９項に記載のパケット送受信装置。

７５．（追加） 前記送信キュー制御手段は、前記第１のパケットまたは前記第２のパケットの送信経路に関する情報と、前記第１のパケットまたは前記第２のパケットを送信するのに必要な帯域幅に関する情報と、前記送信パケットの送信から到着までの遅延に関する情報と、前記第１のパケットまたは前記第２のパケットの優先度に関する情報とのうち少なくとも１つの情報を用いて、前記第１のキュー手段に蓄積された前記第１のパケットおよび前記第２のキュー手段に蓄積された前記第２のパケットのいずれを送信するかを制御する、請求の範囲第５２項に記載のパケット送受信装置。

７６．（追加） 前記送信キュー制御手段は、ＩＥＴＦ ｒｆｃ２２０５、ｒｆｃ２２０８、ｒｆｃ２２０９で記載されたＲＳＶＰ方式、ＩＥＴＦ ｒｆｃ２２１０、ｒｆｃ２２１１、２２１２，ｒｆｃ２２１５で記載されたＩｎｔｓｅｒｖ方式、ＩＥＴＦ ｒｆｃ２４７４、ｒｆｃ２４７５、ｒｆｃ２５９７、ｒｆｃ２５９８で記載されたＤｉｆｆｓｅｒｖ方式のいずれか１つの制御方式を使用する、請求の範囲第７５項に記載のパケット送受信装置。

７７．（追加） 前記送信キュー制御手段は、前記第１のキュー手段に蓄積された前記第１のパケットおよび前記第２のキュー手段に蓄積された前記第２のパケットのうちのいずれかを選択して、選択したパケットを優先的に出力するように前記第１のキュー手段および前記第２のキュー手段を制御する、請求の範囲第５２項に記載のパケット送受信装置。

７８．（追加） 前記送信キュー制御手段は、前記第１のキュー手段から送信さ

れる前記第１のパケットと前記第２のキュー手段から送信される前記第２のパケットとの間隔を平均化するように前記第１のキュー手段および前記第２のキュー手段を制御する、請求の範囲第５２項に記載のパケット送受信装置。

７９．（追加） 前記送信条件設定管理手段および前記受信条件設定管理手段は、前記送信フレームの送信から到着するまでの間において前記送信パケットの送信先から受信先までの経路における最大伝送パケットサイズの検出を行ない、前記最大伝送パケットサイズ情報を用いて、前記送信条件設定情報および前記受信条件設定情報を生成する、請求の範囲第５２項に記載のパケット送受信装置。

８０．（追加） 前記フレーム化手段は、前記パケット化手段にて生成された前記送信パケットに、ＩＥＥＥ ８０２．３規格のフレームヘッダを付加する、請求の範囲第５２項に記載のパケット送受信装置。

８１．（追加） 前記フレーム化手段は、前記パケット化手段にて生成された前記送信パケットに、ＩＥＥＥ ８０２．１Ｑ規格のフレームヘッダを付加する、請求の範囲第５２項に記載のパケット送受信装置。

８２．（追加） 前記パケット化手段は、前記暗号化送信データを所定の大きさに変換し、ＩＥＴＦでＩＰｖ４またはＩＰｖ６として規定されているＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）ヘッダを付加する、請求の範囲第５２項に記載のパケット送受信装置。

８３．（追加） 前記パケット化手段は、ＩＰｖ４ヘッダのサービスタイプフィールド、または、サービスタイプフィールド内のＴＯＳ（Ｔｙｐｅ ｏｆ Ｓｅｒｖｉｃｅ）フィールドに優先パケットであることを示す情報を付加する、請求

の範囲第５２項に記載のパケット送受信装置。

８４．（追加） 前記パケット化手段は、ＩＰｖ６ヘッダのプライオリティフィールドに優先パケットであることを示す情報を付加する、請求の範囲第５２項に記載のパケット送受信装置。

８５．（追加） 前記認証・鍵交換手段は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可する、請求の範囲第５２項に記載のパケット送受信装置。

８６．（追加） 前記送受信管理情報は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報との少なくとも一方を含んでいる、請求の範囲第８５項に記載のパケット送受信装置。

８７．（追加） 前記位置情報は、地域コード、住所、郵便番号、または、経度・緯度により範囲が指定された情報である、請求の範囲第８６項に記載のパケット送受信装置。

８８．（追加） 前記認証・鍵交換手段は、

前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間で認証を行った場合に、前記送信パケットの到着先または前記受信パケットの送信元に関する情報を一時的に記憶する記憶手段と、

前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元とが前記あらかじめ決められた条件に合致しないために前記認証が成

立しない場合に、前記記憶手段にて記憶された情報と、前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報とを照合し、前記パケット送受信装置と前記送信パケットの到着先または前記受信パケットの送信元との間で認証を行う、照合手段と

を含む、請求の範囲第８５項に記載のパケット送受信装置。

８９．（追加） 前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報は、証明書、ＭＡＣアドレスおよび生体情報の少なくとも１つを含む、請求の範囲第８８項に記載のパケット送受信装置。

９０．（追加） 前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期間で暗号化鍵または復号鍵を更新する、請求の範囲第５２項に記載のパケット送受信装置。

９１．（追加） 前記認証・鍵交換手段が前記復号鍵を更新するタイミングを示すタイミング情報が、前記送信パケットに付加される、請求の範囲第９０項に記載のパケット送受信装置。

９２．（追加） 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、一定のデータ量毎に変化される、請求の範囲第９０項に記載のパケット送受信装置。

９３．（追加） 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＲＴＰを使用している場合、予め決められた期間内に更新される、請求の範囲第９０項に記載のパケット送受信装置。

９４．（追加） 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも１つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

前記復号鍵を用いて前記受信データを復号する復号手段と

を備え、

前記認証・鍵交換手段は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可し、

前記認証・鍵交換手段は、前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間で、前記パケット送受信装置から前記送信パケットの到着先または前記受信パケットの受信元までの片道または往復

の伝播時間があらかじめ決められた制限時間より短い時間である場合に、認証を許可する、パケット送受信装置。

９５．（追加） 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも１つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

前記復号鍵を用いて前記受信データを復号する復号手段と

を備え、

前記認証・鍵交換手段は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可し、

前記認証・鍵交換手段は、前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間の送受信区間において無線伝送区間が存在する場合、前記無線伝送区間ではデータをスクランブルして伝送するモードであることを確認した場合に、認証を許可する、パケット送受信装置。

９６．（追加） 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも１つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

前記復号鍵を用いて前記受信データを復号する復号手段と

を備え、

前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期

間で暗号化鍵または復号鍵を更新し、

前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットのＴＣＰポート番号、またはＵＤＰポート番号を変化させることによって通知される、パケット送受信装置。

９７．（追加） 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも１つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

前記復号鍵を用いて前記受信データを復号する復号手段と

を備え、

前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期

間で暗号化鍵または復号鍵を更新し、

前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、ＨＴＴＰリクエスト毎に更新される、パケット送受信装置。

９８．（追加）　送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも１つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

前記復号鍵を用いて前記受信データを復号する復号手段と

を備え、

前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期

間で暗号化鍵または復号鍵を更新し、

前記認証・鍵交換手段がＤＴＣＰ方式の場合、コピー制御情報は、前記送信パケットに暗号化モード情報を付加することによって伝送される、パケット送受信装置。

Translation

PATENT COOPERATION TREATY

PCT/JP2003/013218

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P32091-P0	FOR FURTHER ACTION See Form PCT/IPEA/416	
International application No. PCT/JP2003/013218	International filing date (*day/month/year*) 15 October 2003 (15.10.2003)	Priority date (*day/month/year*) 17 October 2002 (17.10.2002)
International Patent Classification (IPC) or national classification and IPC H04L 12/56, 9/00		
Applicant MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

3. This report is also accompanied by ANNEXES, comprising:

   a. ☒ *(sent to the applicant and to the International Bureau)* a total of 18 sheets, as follows:

      ☒ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

      ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) _____, containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

   ☒ Box No. I Basis of the report
   ☐ Box No. II Priority
   ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   ☒ Box No. IV Lack of unity of invention
   ☐ Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   ☐ Box No. VI Certain documents cited
   ☐ Box No. VII Certain defects in the international application
   ☐ Box No. VIII Certain observations on the international application

Date of submission of the demand 05 February 2004 (05.02.2004)	Date of completion of this report 20 May 2004 (20.05.2004)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/JP2003/013218

Box No. I Basis of the report

1. With regard to the language, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ This report is based on translations from the original language into the following language _____, which is language of a translation furnished for the purpose of:

- ☐ international search (under Rules 12.3 and 23.1(b))
- ☐ publication of the international application (under Rule 12.4)
- ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

☐ The international application as originally filed/furnished

☒ the description:

pages 1-76, as originally filed/furnished
pages* _____ received by this Authority on _____
pages* _____ received by this Authority on _____

☒ the claims:

pages _____, as originally filed/furnished
pages* _____, as amended (together with any statement) under Article 19
pages* 52-98 received by this Authority on 14 May 2004 (14.05.2004)
pages* _____ received by this Authority on _____

☒ the drawings:

pages 1-38, as originally filed/furnished
pages* _____ received by this Authority on _____
pages* _____ received by this Authority on _____

☐ a sequence listing and/or any related table(s) – see Supplemental Box Relating to Sequence Listing.

3. ☒ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☒ the claims, Nos. 1-51
- ☐ the drawings, sheets/figs _____
- ☐ the sequence listing *(specify)*: _____
- ☐ any table(s) related to sequence listing *(specify)*: _____

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/figs _____
- ☐ the sequence listing *(specify)*: _____
- ☐ any table(s) related to sequence listing *(specify)*: _____

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/JP03/13218

Box No. V **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	52-98	YES
	Claims		NO
Inventive step (IS)	Claims	68, 70, 71, 74, 94-98	YES
	Claims	52-67, 69, 72, 73, 75-93	NO
Industrial applicability (IA)	Claims	52-98	YES
	Claims		NO

2. Citations and explanations (Rule 70.7)

Document 1: JP, 2002-202720, A (Toshiba Corporation), July 19, 2002 (07.19.02), Abstract

Document 2: JP, 2000-341324, A (NTT Data Corporation), December 8, 2000 (12.08.00), Paragraph Nos. [0002] and [0003]

Document 3: JP, 7-79252, A (Fujitsu Limited), March 20, 1995 (03.20.95), Abstract

Document 4: JP, 8-130543, A (Nippon Telegraph and Telephone Corporation), May 21, 1996 (05.21.96), Abstract

Document 5: JP, 2000-299686, A (NEC Corporation), October 24, 2000 (10.24.00), Abstract

Document 6: JP, 2002-26906, A (Mitsubishi Electric Corporation), January 25, 2002 (01.25.02), Paragraph Nos. [0036] and [0037]

Document 7: JP, 7-297831, A (Sumitomo Electric Industries, Ltd.), November 10, 1995 (11.10.95), Paragraph No. [0038]

Document 8: Manabu TAKADA, Yoshihisa MIWA, "Tokushu 2, Internet no Kiban "IP wo Shiru," Nikkei Network, Nikkei BP, Vol. 30, September 22, 2002 (09.22.02), pp.124-139, "Yakuwari 3, Packet wo Bunkatsu suru Toru Kaisen ni Awasete Okisa wo Chosei," (pp.132-135)

Document 9: JP, 11-196081, A (K.K. Kodo Idotsushin Security Gijutsu Kenkyusho), July 21, 1999 (07.21.99), Paragraph No. [0003]

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of Box V.2:

Document 10: Yoshikazu YAMAMOTO, Kenichi NISHINO, Tetsuya TAKAHASHI, "Tsushin Cost Sakugen no Buki to shite no VPN," Interop Magazine, Soft Bank Publishing Kabushiki Kaisha, Vol.9, No.8, October 1, 1999 (10.01.99), pp.44-51, p.48, left column, lines 32 to 35

Document 11: JP, 2002-217961, A (Fujitsu Limited), August 2, 2002 (08.02.02), Claim 2

Document 12: JP, 2001-186173, A (Matsushita Electric Industrial Co., Ltd.), July 6, 2001 (07.06.01), Paragraph No. [0153]

Document 13: JP, 2002-232955, A (Denso Corporation), August 16, 2002 (08.16.02), Claims 1-3

Document 14: JP, 2001-86110, A (Toyo Communication Equipment Co., Ltd.), March 30, 2001 (03.30.01), Paragraph No. [0005], Fig. 9

Claims 52-54, 65-67, 75-77 and 80-82

Each of the above documents 1 and 2 describes key exchange between a transmission device and reception device, and based on the key exchanged by the key exchange, encrypting the data, and transmitting and receiving the same.

Also, using transmission-related information such as a sending address and transmission/reception managing information such as a MAC address to generate a packet is generally carried out in an IP network.

Also, documents 3 and 4 describe that, when buffer storage capacity exceeds threshold, data in the buffer is preferentially output.

When storage capacity exceeds a threshold, controlling by preferentially outputting data so that storage capacity declines below the threshold is the same as controlling so that storage capacity does not exceed the threshold.

Document 5 describes accumulating packets in a plurality of class queues, and in accordance with bandwidth information allocated to the class, outputting the packets accumulated in each queue.

Claims 55-64

Document 6 describes transmitting important data encrypted and data of low important without encryption.

Controlling the data transmission rate of data so as not to decline below a prescribed value is generally carried out in shaping and the like.

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of Box V.2:

Claim 60

Document 7 describes outputting data so as not to exceed remaining accumulation time, that is, outputting data so that the accumulation time is shorter than a value set in advance.

Claims 61-64 and 79

Document 8 describes checking the maximum transmissible packet length in a transmission route from transmission device to reception device, and transmitting data at maximum packet length.

Attaching to a packet data on packet length for transmission and data for error correction is generally carried out.

Claim 69, 73, 90 and 93

Document 9 describes that when a key has been used for a prescribed time, the key is updated.

Under what protocols a key is to be updated every set time frame is a matter of design that could be determined as appropriate by a party skilled in the art, and no particular difficulty is found in adopting a known RTP as a protocol.

Claims 72 and 92

Document 10 describes updating a key for every time a set volume of data is processed.

Under what protocols a key is to be updated for every time a set volume of data is processed is a matter of design that could be determined as appropriate by a party skilled in the art, and no particular difficulty is found in adopting a known HTTP as a protocol.

Claim 78

Document 11 describes outputting packets evenly from a plurality of queues.

Claims 83 and 84

Document 12 describes using a TOS field for an Ipv4 packet and a traffic class field for an Ipv6 packet as fields for packet priority.

Claims 85-89

Document 13 describes performing authentication in accordance with position information of a mobile terminal, and if authentication is denied, performing authentication using a password.

A constitution such that authentication is made using a certificate or and the like in place of authentication using a password could be easily conceived of by a party skilled in the art.

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of Box V.2:

Claim 91

Document 14 describes adding key change timing to a transmission packet.

Claim 68

None of the above documents 1-14 describes or suggests transmitting information indicating encryption key prior to the time from transmission of a transmission frame to reception of a reception frame corresponding thereto.

Claims 70, 71, 74, 96 and 97

None of the above documents 1-14 describes or suggests setting key update timing to be timing synchronized to a sequence number, updating each HTTP request, setting a timing synchronized to an end or beginning of an error correction matrix, and notifying timing by a port number change.

Claims 94 and 95

None of the above documents 1-14 describes or suggests performing authentication in accordance with one way or round-trip propagation delay time of a packet, and whether the mode is scrambled transmission.

Claim 98

None of the above documents 1-14 describes or suggests transmitting DTCP system copy control information by adding encryption mode information to a transmission packet.